Nuevos protocolos de consulta de DNS (DoH y DoT)

48º GGTT RedIRIS

Valladolid, 28 de noviembre de 2019

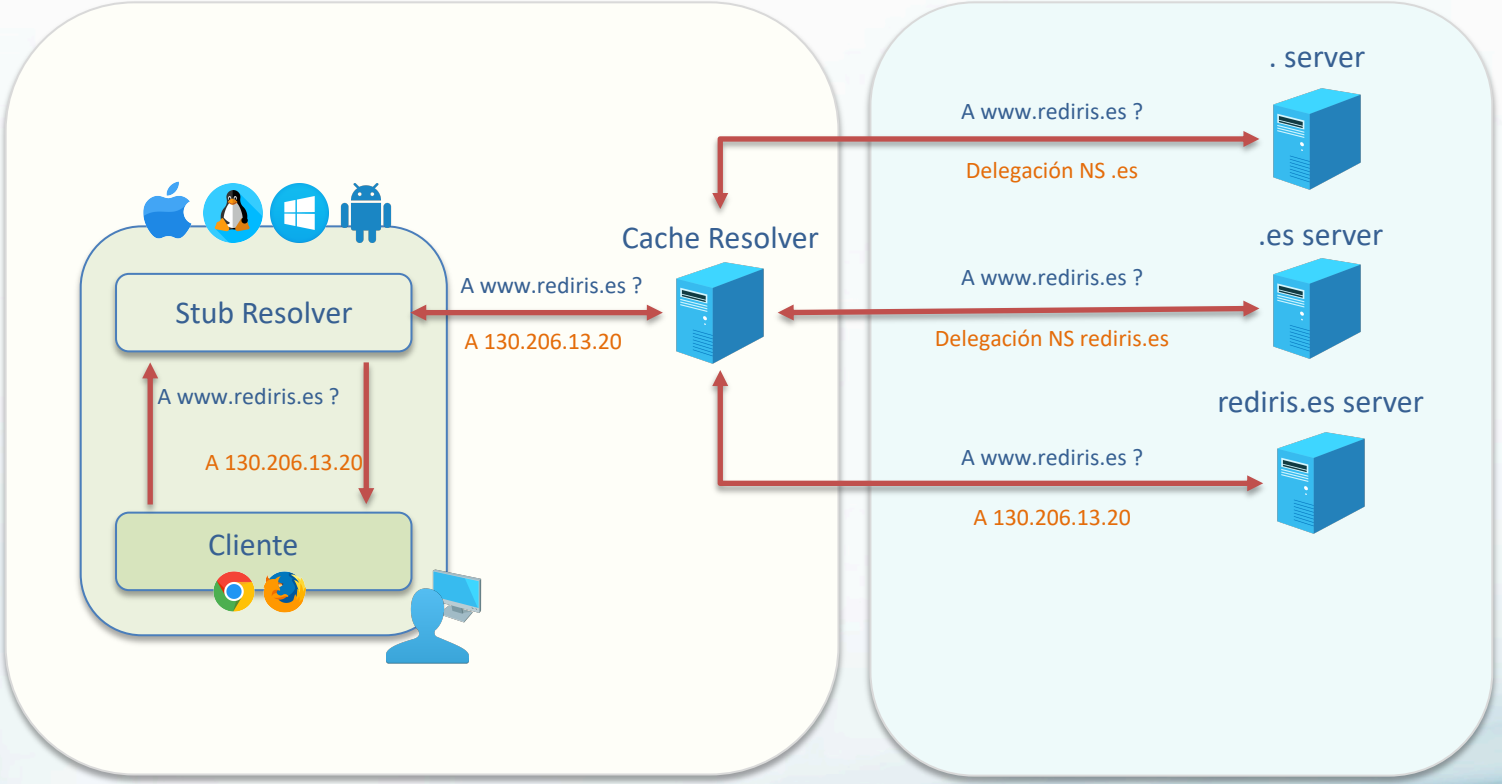
Juan Carlos Rodríguez

Jcarlos.rodriguez@rediris.es

RedIRIS

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
MINISTERIO DE ECONOMÍA Y EMPRESA
RedIRIS
red.es
Infraestructuras Científicas y Técnicas Singulares

Las dos vistas del DNS: recursivo vs autoritativo



Las dos vistas del DNS: autoritativo

- Objetivo
  - Publicar dominios
- Elementos
  - Primario: contiene la zona original
  - Secundario: publica una copia
- Seguridad
  - Arquitectura primario oculto: protección de los datos originales
  - Firmado DNSSEC: integridad respuestas
  - Publicación Anycast: protección frente a DDoS
  - TSIG: protege la comunicación primario-secundario

Las dos vistas del DNS: recursivo

- Objetivo
  - Resolver dominios
- Elementos
  - Aplicación cliente
  - Stub resolver
  - Recursive Caching resolver
- Seguridad
  - DNS firewall: protección usuarios vs Malware, Phising, Botnets
  - Validación DNSSEC: autenticidad de la respuesta
  - ¿DoT y DoH?: privacidad y confidencialidad

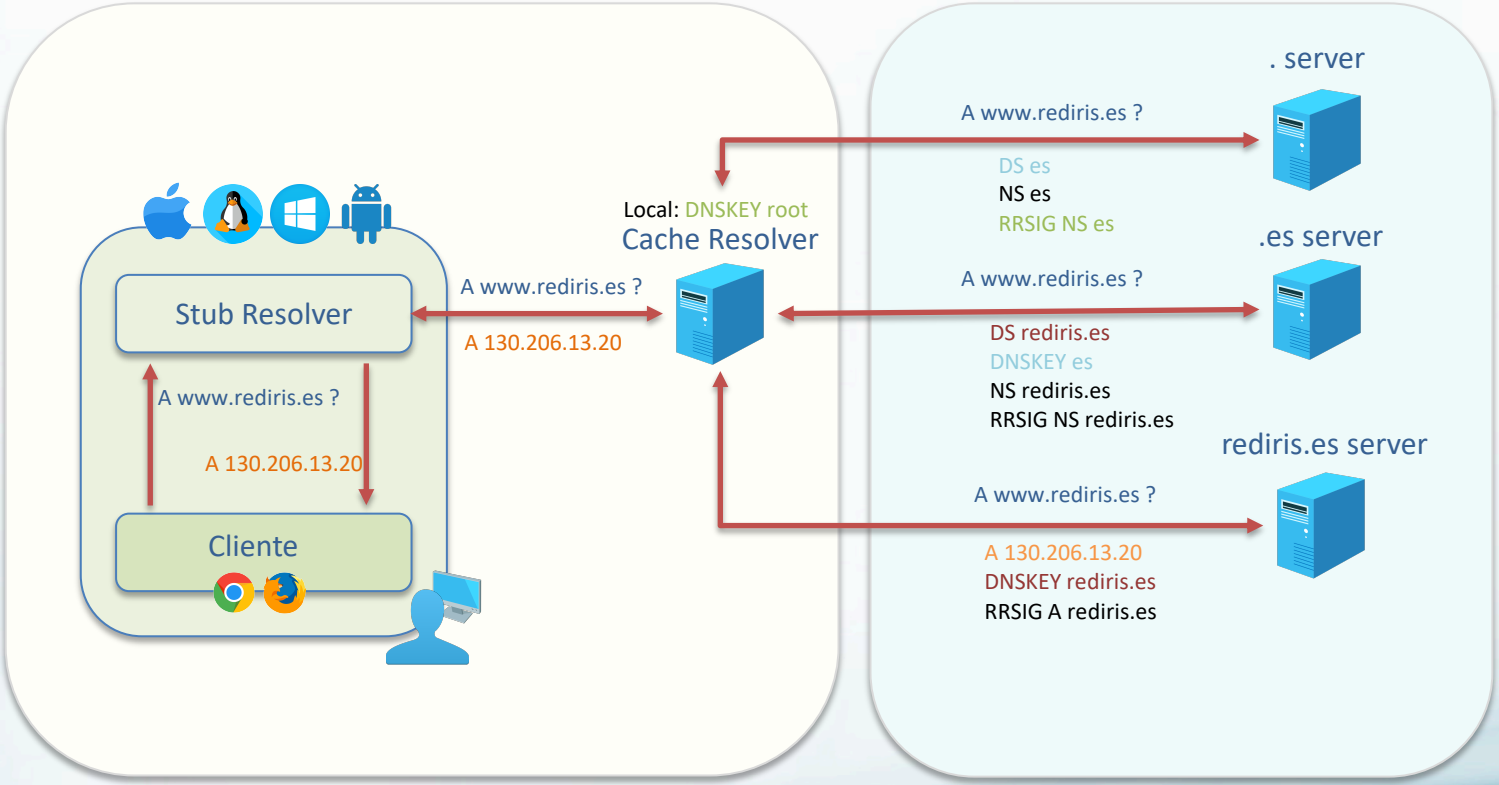
Problema de seguridad en DNS: ultima milla

- Las consultas entre el cliente y el resolver son en texto plano
  - Ataques man-in-the-middle
  - Inspección de paquetes (legítimas y no legítimas)
- DoH y DoT cifran la comunicación entre el cliente y el resolver

No es DNSSEC

- DNSSEC es usado en los mensajes entre el servidor autoritativo y el resolver
  - Transparente para el cliente
  - Compatible con versiones anteriores de DNS
- DNSSEC verifica la autenticidad e integridad de la respuesta
  - Nuevas funcionalidades: DANE
- DNSSEC no usa cifrado
  - No añade privacidad ni confidencialidad
- DNSSEC todavía en etapa de adopción

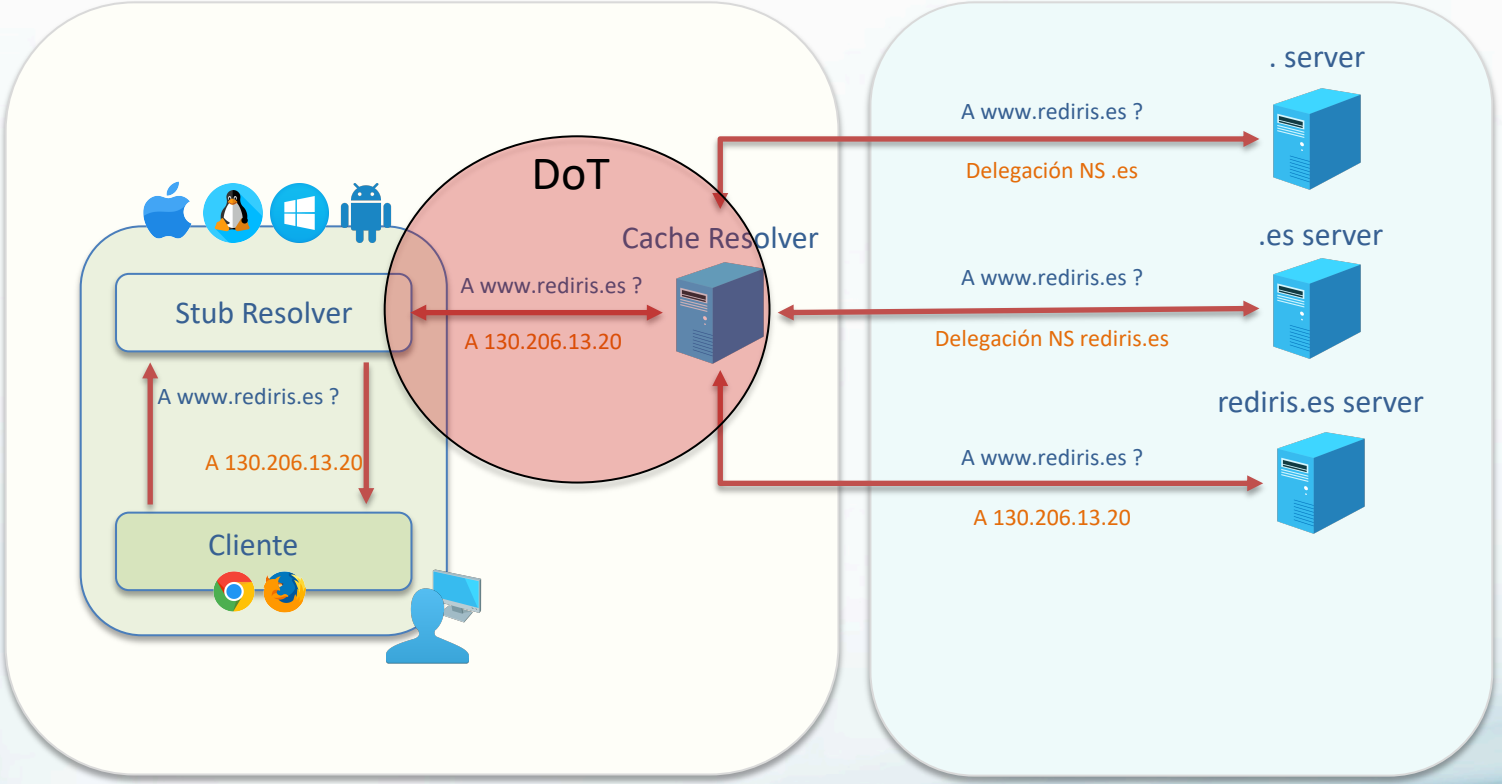
No es DNSSEC


Stub Resolver
A www.rediris.es ?
A 130.206.13.20
Cliente
A www.rediris.es ?
A 130.206.13.20
Local: DNSKEY root
Cache Resolver
. server
A www.rediris.es ?
DS es
NS es
RRSIG NS es
.es server
A www.rediris.es ?
DS rediris.es
DNSKEY es
NS rediris.es
RRSIG NS rediris.es
rediris.es server
A www.rediris.es ?
A 130.206.13.20
DNSKEY rediris.es
RRSIG A rediris.es

DoT

- DNS over TLS
- RFC7858: Specification for DNS over Transport Layer Security (TLS)
  - https://datatracker.ietf.org/doc/rfc7858/
- Usa un puerto dedicado (853), es bloqueable
  - Es ”compatible con versiones anteriores de DNS”
- Cifra la comunicación entre el stub resolver y el resolver
  - Los SO aún no lo implementan (excepto Android 9)
- Añade privacidad y confidencialidad

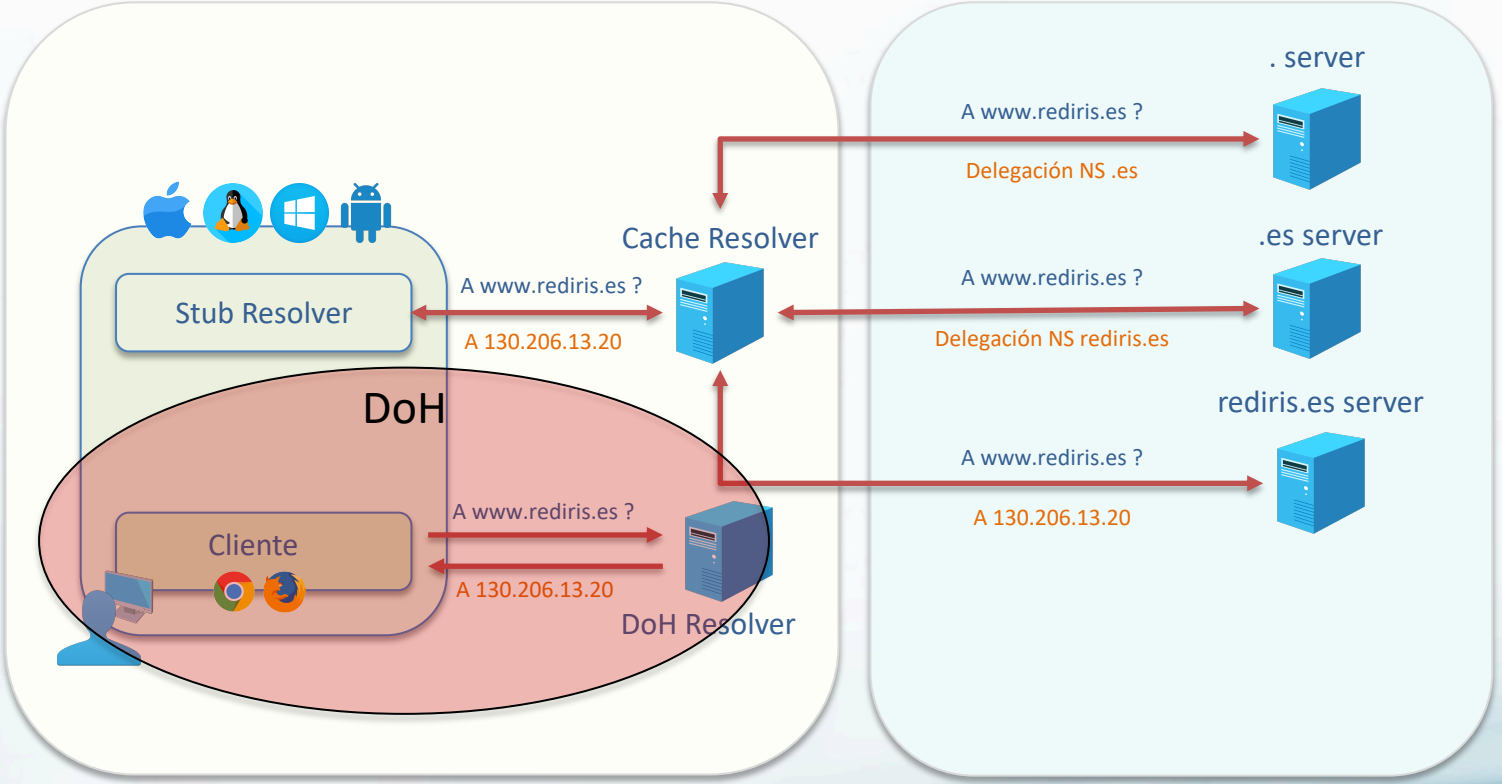
DoT


DoT
Cache Resolver
Stub Resolver
A www.rediris.es ?
A 130.206.13.20
A www.rediris.es ?
A 130.206.13.20
Cliente
. server
A www.rediris.es ?
Delegación NS .es
.es server
A www.rediris.es ?
Delegación NS rediris.es
rediris.es server
A www.rediris.es ?
A 130.206.13.20

DoH

- DNS over HTTPS
- RFC8484: DNS Queries over HTTPS (DoH)
  - https://datatracker.ietf.org/doc/rfc8484/
- Implementado directamente en los navegadores
- NO es ”compatible con versiones anteriores de DNS”
  - Usa un puerto compartido (443), no es fácilmente bloqueable
  - No usa el resolver del ISP o el sistema operativo
  - Cifra la comunicación entre el navegador y el resolver seleccionado
- Añade privacidad y confidencialidad
- Potencialmente DISRUPTOR

DoH


. server
A www.rediris.es ?
Delegación NS .es
Cache Resolver
.es server
Stub Resolver
A www.rediris.es ?
A 130.206.13.20
A www.rediris.es ?
Delegación NS rediris.es
rediris.es server
DoH
A www.rediris.es ?
A 130.206.13.20
Cliente
A www.rediris.es ?
A 130.206.13.20
DoH Resolver

DoH: ejemplo

```
atlas:~ jcarlos$ curl -s -H 'accept: application/dns+json'
'https://dns.google.com/resolve?name=red.es&type=A'

{
"Status": 0,"TC": false,"RD": true,"RA": true,"AD": false,"CD": false,
"Question":[ {"name": "red.es.","type": 1}],
"Answer":[
 {"name": "red.es.", "type": 1, "TTL": 59, "data": "13.224.106.44" },
 {"name": "red.es.","type": 1,"TTL": 59,"data": "13.224.106.45"},
 {"name": "red.es.","type": 1,"TTL": 59,"data": "13.224.106.115"},
 {"name": "red.es.","type": 1,"TTL": 59,"data": "13.224.106.37"}
 ],
 "Comment": "Response from 205.251.192.177."
}
```

```
atlas:~ jcarlos$ dig A red.es @8.8.8.8

; <<>> DiG 9.8.3-P1 <<>> A red.es @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29291
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;red.es.                        IN      A

;; ANSWER SECTION:
red.es.         59      IN      A       13.224.106.44
red.es.         59      IN      A       13.224.106.45
red.es.         59      IN      A       13.224.106.115
red.es.         59      IN      A       13.224.106.37

;; Query time: 30 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Nov 25 12:09:07 2019
;; MSG SIZE  rcvd: 88
```

DoH Problemas/polémica

Cifrado + resolver fuera de la organización/ISP + puerto compartido = Muchos problemas

- El tráfico cifrado DNS por si mismo no es un problema
- Resolver distinto al del ISP/organización
  - Resoluciones privadas no resolubles por el cliente
  - CDN: no es posible seleccionar el mejor nodo de contenidos
  - Soluciones de seguridad ineficientes
    - El DNS es información relevante de seguridad
    - Políticas de protección/filtrado/judiciales/parentales esquivadas
- Tráfico indistinguible de HTTPS
  - No bloqueable/detectable fácilmente

DoH Debate abierto

DNS-over-HTTPS causes more problems than it solves, experts say
https://www.zdnet.com/article/dns-over-https-causes-more-problems-than-it-solves-experts-say/

UK ISP group names Mozilla 'Internet Villain' for supporting 'DNS-over-HTTPS'
https://www.ispa.org.uk/ispa-announces-finalists-for-2019-internet-heroes-and-villains-trump-and-mozilla-lead-the-way-as-villain-nominees/

The U.S. House Judiciary Committee Is Investigating Google's Plans to Implement DNS Over HTTPS
http://www.circleid.com/posts/20190930_us_house_judiciary_committee_investigating_googles_doh_plans

https://www.ncta.com/media/media-room/ncta-ctia-and-ustelecom-alert-congressional-committees-about-googles-new-browser-protocol

Windows will improve user privacy with DNS over HTTPS
https://techcommunity.microsoft.com/t5/Networking-Blog/Windows-will-improve-user-privacy-with-DNS-over-HTTPS/ba-p/1014229

This DNS over HTTP thing (NANOG archives)
https://mailman.nanog.org/pipermail/nanog/2019-October/103204.html

….. Y sigue ….

DoH Estado de desarrollo y despliegue (clientes)

Google y Mozilla han sido los impulsores iniciales y ante las críticas han ido ”matizando” la implementación en Chrome y Firefox

- Chrome (https://www.chromium.org/developers/dns-over-https)
  - Respetará el resolver del SO, si soporta DoH, cambiará de DNS plano a DoH

- Firefox (https://support.mozilla.org/en-US/kb/configuring-networks-disable-dns-over-https)
  - Activado por defecto en el futuro. Proveerá una serie de mecanismos para conocer si el entorno es “compatible” con DoH y deshabilitarlo
    - Canaray domain, security.enterprise_roots.enabled, parental control…
  - Pero... el usuario puede usar DoH sin respetar ninguna otra consideración si lo configura explícitamente

- Microsoft ha anunciado soporte en Windows 10 para DoH (y en el futuro DoT)

DoH Estado de desarrollo y despliegue (servidores)

- https://github.com/curl/curl/wiki/DNS-over-HTTPS

- Cloudfare https://cloudflare-dns.com/dns-query
- Google https://dns.google/dns-query
- Opendns https://doh.opendns.com/dns-query
- Quad9 https://dns.quad9.net/dns-query
- ….

- BIND soportará DoH y DoT nativamente en 2020
- Ubound soporta nativamente DoT
- PowerDNS (dnsdist) soporta DoT y DoH (https://doh.powerdns.org/)
- ….

Recomendaciones

NCSC: Factsheet DNS monitoring will get harder
https://english.ncsc.nl/publications/factsheets/2019/oktober/2/factsheet-dns-monitoring-will-get-harder

“The NCSC recommends organisations to decide on preferred (DNS) resolvers, configure these on devices under administrative control and take note of the benefits provided by modern DNS transport protocols.”

“ Take into account the level of access provided to unmanaged clients, the risks this entails and the required trade-off for guest and private use when deciding to accept or mitigate.“

¡Muchas gracias!

Más de 25 años al servicio de la investigación